(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2015-176167
(P2015-176167A)
(43)公開日　平成27年10月5日(2015.10.5)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/31	(2013.01)	G06F	21/20	131A	5J104
G06F 21/44	(2013.01)	G06F	21/20	144C	
H04L 9/32	(2006.01)	G06F	21/20	144D	
G09C 1/00	(2006.01)	H04L	9/00	675B	
		G09C	1/00	640E	

審査請求 有　請求項の数 9　ＯＬ　外国語出願　（全 12 頁）

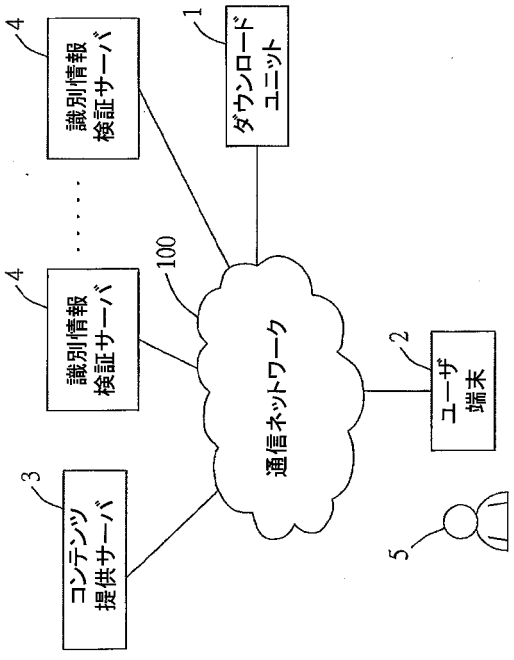
(21)出願番号　特願2014-49573(P2014-49573)
(22)出願日　平成26年3月13日(2014.3.13)

(71)出願人　511022096
キーパスコ　アーベー
Ｋｅｙｐａｓｃｏ　ＡＢ
スウェーデン，エスイー－４１１　ゴッテンブルグ　１５
ＳＥ－４１１　１５　Ｇｏｔｈｅｎｂｕｒｇ，Ｓｗｅｄｅｎ
(74)代理人　100096091
弁理士　井上　誠一
(72)発明者　林　茂聰
台湾台北市内湖區内湖路二段１０３巷１０３之１號９樓
(72)発明者　ペール　スキゲブイェルグ
スウェーデン　ゴッテンブルグ　エスイー－４１１　１８　マガシンスガタン　２４

Ｆターム(参考)　5J104 AA07　KA05　PA07

(54)【発明の名称】ユーザ識別情報を安全に検証するためのネットワーク認証方法

(57)【要約】
【課題】ユーザの識別情報を安全に検証するためのネットワーク認証方法を提供する。
【解決手段】ネットワーク認証方法において、コンテンツ提供サーバ（３）はダウンロードユニット（１）からダウンロードした非対称秘密鍵によって署名された暗号化されたウェブアドレスを識別情報検証サーバ（４）から取得するため、ユーザ端末(２)を識別情報検証サーバ（４）へリダイレクトする。ユーザ端末（２）は、ダウンロードユニット（１）からダウンロードした暗号化されたウェブアドレス及び非対称公開鍵に基づき、識別情報検証サーバ（４）が、現在、識別情報を検証するために有効であると判定されると、ユーザ端末（２）に紐づくハードウェアスキャンデータを識別情報検証サーバへ送信する。識別情報検証サーバ（４）は、ハードウェアスキャンデータ及び予め記憶された参照ハードウェアスキャンデータとの関連に基づき、ユーザ端末（２）の識別情報を検証する。
【選択図】図１



【特許請求の範囲】
【請求項１】
ユーザ端末、ダウンロードユニット、コンテンツ提供サーバ、及び前記ユーザ端末のユーザ識別情報を安全に検証するための複数の識別情報検証サーバにより実行されるネットワーク認証方法であって、
ａ）前記ユーザ端末は、前記ダウンロードユニットから、スキャンプログラム、及び非対称公開鍵をダウンロードするステップａ）と、
ｂ）各々の前記識別情報検証サーバは、非対称秘密鍵によって署名され、暗号化された前記識別情報検証サーバのウェブアドレスを含む各々の暗号化情報のセットを、ダウンロードユニットからダウンロードし、前記ユーザ端末に紐づき前記ユーザのユーザ識別子と一意に対応する参照ハードウェアスキャンデータを記憶するステップｂ）と、
ｃ）前記コンテンツ提供サーバへアクセスするための前記ユーザ端末からのユーザログイン要求に応答し、前記コンテンツ提供サーバは、第１の通信リンクを介して、１つの前記識別情報検証サーバに、前記ユーザの前記識別情報が検証を要する検証通知を送信し、第２の通信リンクを介して、当該１つの前記識別情報検証サーバと接続するために前記ユーザ端末をリダイレクトするステップｃ）と、
ｄ）当該１つの前記識別情報検証サーバは、前記第２の通信リンクを介して、前記ユーザ端末に、ステップｂ）においてダウンロードした前記各々の暗号化情報のセットを送信するステップｄ）と、
ｅ）前記ユーザ端末は、少なくともステップｄ）において送信された前記各々の暗号化情報のセット、及びステップａ）においてダウンロードした非対称公開鍵に基づき、当該１つの前記識別情報検証サーバが、現在、識別情報を検証するために有効か否かを判定するステップｅ）と、
ｆ）当該１つの前記識別情報検証サーバは、現在、識別情報を検証するために有効であると判定すると、前記ユーザ端末は、前記ユーザ端末に紐づくハードウェアスキャンデータを取得するために、ステップａ）においてダウンロードしたスキャンプログラムを実行し、前記第２の通信リンクを介して、取得した前記ハードウェアスキャンデータを、当該１つの前記識別情報検証サーバへ送信するステップｆ）と、
ｇ）当該１つの前記識別情報検証サーバは、ステップｆ）において前記ユーザ端末から受信した前記ハードウェアスキャンデータとステップｂ）において記憶した前記参照ハードウェアスキャンデータとの関連に基づき、前記ユーザの前記識別情報の検証をし、コンテンツ提供サーバへ検証結果を通知するステップｇ）と、
を含むことを特徴とするネットワーク認証方法。
【請求項２】
前記ユーザ端末は、各々一意な識別コードを有する複数のハードウェアコンポーネントを含み、ステップａ）とステップｂ）との間に、更に、
前記ユーザ端末は、前記参照ハードウェアスキャンデータとして機能する各々の前記ハードウェアコンポーネントの前記識別コードを取得するために、前記ユーザ端末の前記ハードウェアコンポーネントをスキャンするための前記スキャンプログラムを実行し、前記参照ハードウェアスキャンデータを、ステップｂ）において記憶するため各々の前記識別情報認証サーバへ送信するステップを含むことを特徴とする請求項１に記載のネットワーク認証方法。
【請求項３】
前記ユーザ端末を前記コンテンツ提供サーバに登録する間、
前記ユーザ端末は、ステップａ）において、前記ダウンロートユニットから、前記スキャンプログラム、及び前記非対称秘密鍵をダウンロードし、ステップｂ）において、各々の前記識別情報検証サーバは、前記ダウンロートユニットから各々の前記暗号化情報をダウンロードし、前記参照ハードウェアスキャンデータを記憶することを特徴とする請求項２に記載のネットワーク認証方法。
【請求項４】

ステップｃ）において、当該１つの前記識別情報検証サーバは、前記コンテンツ提供サーバによって決定されることを特徴とする請求項１に記載のネットワーク認証方法。
【請求項５】
ステップｃ）において、当該１つの前記識別情報検証サーバは、前記ユーザ端末によって決定されることを特徴とする請求項１に記載のネットワーク認証方法。
【請求項６】
ステップｃ）において、
ｃ１）前記ユーザ端末からの前記ログイン要求に応答し、前記コンテンツ提供サーバは、前記ユーザ端末に、各々の前記識別情報検証サーバを表す選択項目のリストを含む選択要求を送信するサブステップｃ１）と、
ｃ２）前記コンテンツ提供サーバは、前記ユーザ端末から、当該１つの前記識別情報検証サーバを表す、要求された１つの前記選択項目を示す選択応答を受信するサブステップｃ２）と、
ｃ３）前記コンテンツ提供サーバは、前記ユーザ端末からの選択応答に従って、当該１つの前記識別情報検証サーバと接続するために、前記ユーザ端末をリダイレクトするサブステップｃ３）と、
を含むことを特徴とする請求項５に記載のネットワーク認証方法。
【請求項７】
ステップｅ）において、
前記ユーザ端末は、前記非対称公開鍵を使用し、暗号化されたウェブアドレスを復号でき、前記暗号化されたウェブアドレスの復号が成功すると、前記ユーザ端末は、当該１つの前記識別情報認証サーバが、現在、識別情報を検証するために有効であると判定することを特徴とする請求項１に記載のネットワーク認証方法。
【請求項８】
ステップｂ）において、各々の前記識別情報認証サーバによりダウンロードした各々の前記暗号化情報のセットは、更に、前記識別情報認証サーバに紐づく暗号化された認証期間を含み、
ステップｅ）は、更に、
ｅ１）前記ユーザ端末は、前記非対称公開鍵を使用し、当該１つの前記識別情報認証サーバに紐づく、前記暗号化されたウェブアドレス及び前記暗号化された認証期間が、正しく復号されたか否かを判定するサブステップｅ１）と、
ｅ２）前記暗号化されたウェブアドレス及び前記暗号化された認証期間の復号に成功すると、前記ユーザ端末は、現在の日付が、当該１つの前記識別情報認証サーバに紐づく復号化された認証期間内か否かを判定するサブステップｅ２）と、
ｅ３）現在の日付が、当該１つの前記識別情報認証サーバと紐づく復号化された認証期間内と判定すると、前記ユーザ端末は、当該１つの前記識別情報認証サーバが、現在、識別情報を検証するために有効であると判定するサブステップｅ３）と、
を含むことを特徴とする請求項１に記載のネットワーク認証方法。
【請求項９】
ステップｅ）において、更に、
ｅ４）現在の日付が、当該１つの前記識別情報認証サーバに紐づく復号化された認証期間外の場合、前記ユーザ端末は、前記ダウンロードユニットに、当該１つの前記識別情報認証サーバと紐づく認証期間が、既に期限が過ぎている旨の期限切れ通知を送信するサブステップｅ４）
を含むことを特徴とする請求項８に記載のネットワーク認証方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワーク識別認証に関し、特にユーザ識別情報を安全に検証するためのネットワーク認証方法に関する。

【背景技術】
【０００２】
現在、クラウドサービスのような様々なインターネットサービスが、ますます普及しつつある。このようなインターネットサービスをセキュアなものとするために、ユーザ識別情報の認証は必要不可欠である。
【０００３】
しかしながら、インターネットユーザ及びインターネット犯罪の数が増え続け、また、犯罪技術が絶えず進歩しているため、例えば、インターネットコンテンツプロバイダ（ＩＣＰ）は、各ユーザに、公開鍵暗号基盤（ＰＫＩ）証明書を有するＵＳＢデバイス、ＩＣカードやダイナミックトークンなどの身元認証デバイスを提供する必要が生ずる。
【０００４】
このため、個人化、分配、及びトラブルシューティングのための顧客サービスのコストが無視できない。さらに、種々のＩＣＰ毎にユーザＩＤやパスワードを覚える必要があること、また、種々のＩＣＰ毎に異なる識別情報認証デバイスを所有する必要があることは、ユーザにとって非常に不便である。また、種々のＩＣＰに対するユーザ身元認証の投資の重複が生ずるであろう。
【０００５】
関連分野の先行技術は、米国特許第８２００８１１号、米国特許出願公開第２０１１／００７８４３９号、米国特許出願公開第２００６／００８０３５２号において開示されている。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】米国特許第８２００８１１号明細書
【特許文献２】米国特許出願公開第２０１１／００７８４３９号明細書
【特許文献３】米国特許出願公開第２００６／００８０３５２号明細書
【発明の概要】
【発明が解決しようとする課題】
【０００７】
したがって、本発明の目的は、上述した従来技術の問題点を克服する、ユーザの識別情報を安全に検証するためのネットワーク認証方法、を提供することにある。
【課題を解決するための手段】
【０００８】
本発明によれば、ユーザ端末、ダウンロードユニット、コンテンツ提供サーバ、及び前記ユーザ端末のユーザ識別情報を安全に検証するための複数の識別情報検証サーバにより実行されるネットワーク認証方法が提供される。ネットワーク認証方法は、ａ）前記ユーザ端末は、前記ダウンロードユニットから、スキャンプログラム及び非対称公開鍵をダウンロードするステップａ）と、ｂ）各々の前記識別情報検証サーバは、非対称秘密鍵によって署名され、暗号化された前記識別情報検証サーバのウェブアドレスを含む各々の暗号化情報のセットを、ダウンロードユニットからダウンロードし、前記ユーザ端末に紐づき前記ユーザのユーザ識別子と一意に対応する参照ハードウェアスキャンデータを記憶するステップｂ）と、ｃ）前記コンテンツ提供サーバへアクセスするための前記ユーザ端末からのユーザログイン要求に応答し、前記コンテンツ提供サーバは、第１の通信リンクを介して、１つの前記識別情報検証サーバに、前記ユーザの前記識別情報が検証を要する検証通知を送信し、第２の通信リンクを介して、当該１つの前記識別情報検証サーバと接続するために前記ユーザ端末をリダイレクトするステップｃ）と、ｄ）当該１つの前記識別情報検証サーバは、前記第２の通信リンクを介して、前記ユーザ端末に、ステップｂ）においてダウンロードした前記各々の暗号化情報のセットを送信するステップｄ）と、ｅ）前記ユーザ端末は、少なくともステップｄ）において送信された前記各々の暗号化情報のセット、及びステップａ）においてダウンロードした非対称公開鍵に基づき、当該１つの前

記識別情報検証サーバが、現在、識別情報を検証するために有効か否かを判定するステップｅ）と、ｆ）当該１つの前記識別情報検証サーバは、現在、識別情報を検証するために有効であると判定すると、前記ユーザ端末は、前記ユーザ端末に紐づくハードウェアスキャンデータを取得するために、ステップａ）においてダウンロードしたスキャンプログラムを実行し、前記第２の通信リンクを介して、取得した前記ハードウェアスキャンデータを、当該１つの前記識別情報検証サーバへ送信するステップｆ）と、ｇ）当該１つの前記識別情報検証サーバは、ステップｆ）において前記ユーザ端末から受信した前記ハードウェアスキャンデータとステップｂ）において記憶した前記参照ハードウェアスキャンデータとの関連に基づき、前記ユーザの前記識別情報の検証をし、コンテンツ提供サーバへ検証結果を通知するステップｇ）と、を含む。

【図面の簡単な説明】

【０００９】

【図１】本発明の好適な実施形態に係るネットワーク認証方法を実行するために構成されたネットワーク認証システムシステムを示す概略ブロック図である。

【図２】好適な実施形態のネットワーク認証方法の登録処理を示すフローチャートである。

【図３】好適な実施形態のネットワーク認証方法のログイン処理を示すフローチャートである。

【図４】好適な実施形態において、認証情報の検証を実行するために１つの識別情報検証サーバを決定する手続きを示す処理のフローチャートである。

【図５】好適な実施形態において、ユーザ端末が、認証情報の検証を実行するために当該１つの識別情報検証サーバが、現在、有効か否かを判定する手続きを示す処理のフローチャートである。

【発明を実施するための形態】

【００１０】

本発明のその他の特徴や効果は、図面を参照しながら以降に詳述する好適な実施形態において明らかになる。

【００１１】

図１を参照すると、本発明の好適な実施形態によれば、ユーザ５の識別情報を安全に検証するためのネットワーク認証方法を実行するために、ネットワーク認証システムが利用される。

【００１２】

ネットワーク認証システムは、ダウンロードユニット１、ユーザ５が所有するユーザ端末２、コンテンツ提供サーバ３（例えば、インターネットコンテンツプロバイダ又はＩＣＰ）、及び複数の認証情報検証サーバ４を含む。

【００１３】

模範的用途のために、ユーザ端末２は、ユーザ５が所有するノートブックコンピュータ、スマートフォン、ＰＤＡなどのインターネットブラウジングやデータ通信が可能な電子デバイスが好ましい。

【００１４】

ユーザ端末２は、中央処理装置、基本入力／出力システム（ＢＩＯＳ）ユニット、記憶装置、通信インターフェース、マザーボードなどの図示しない複数のハードウェアコンポーネントを含み、各々が一意な識別コードを有する。

【００１５】

コンテンツ提供サーバ３は、ネット銀行サーバ、オンラインゲームサーバ、又はポータルウェブサイトのような識別情報の検証を必要とするネットワークサービスを提供するその他のサーバでよい（但し、これらに限定されない）。

【００１６】

識別情報検証サーバ４は、理想的には、サードパーティ検証を行うためにダウンロードユニット１により許可された、グーグル（登録商標）、ヤフー（登録商標）、フェースブ

ック（登録商標）などのようなソーシャルネットワークのウェブサイトでよい（但し、これらに限定されない）。

【００１７】

ダウンロードユニット１は、少なくとも、１つのスキャンプログラム、１組の非対称公開鍵及び非対称秘密鍵、及び識別情報検証サーバ４の各々に対応する暗号化情報のセットを記憶するための図示しないデータベースユニット、を含む。

【００１８】

各々の暗号化情報のセットは非対称秘密鍵で署名されており、各々対応する１つの識別情報検証サーバ４の暗号化されたウェブアドレスを含む。

【００１９】

特に、各々の暗号化情報のセットは、デジタル署名を生成するために非対称秘密鍵により処理されている。そして、非対称公開鍵は、デジタル署名を検証するために使用される。

【００２０】

ダウンロードユニット１、ユーザ端末２、コンテンツ提供サーバ３、及び識別情報検証サーバ４は、通信ネットワーク１００と接続されている。

【００２１】

図１、２を参照する。ダウンロードユニット１は、ユーザ端末２及びコンテンツ提供サーバ３と協働し、本発明に係る好適な実施形態のネットワーク認証方法の登録処理を実行する。

【００２２】

好適な実施形態のネットワーク認証方法の登録処理は、次のステップを含む。

登録処理の前に、各々の識別情報検証サーバ４は、ダウンロードユニット１から各々の暗号化情報のセットをダウンロードするために、通信ネットワーク１００を介して、ダウンロードユニット１と接続されている点に留意すべきである。

【００２３】

ステップＳ２１において、ユーザ５は、コンテンツ提供サーバ３が提供するウェブサイト上で、図示しないユーザ入力インターフェースを用いて、ユーザ識別子として機能するユーザＩＤ及びパスワードを入力する。そして、ユーザＩＤ及びパスワードは、通信ネットワーク１００を介して、ユーザ端末２からコンテンツ提供サーバ３へ送信される。

【００２４】

ステップＳ２２において、ユーザＩＤ及びパスワードの受信に応答して、コンテンツ提供サーバ３は、ユーザＩＤ及びパスワードが正しいか否かをチェックする。

正しければ、ステップＳ２３に進む。そうでなければ、コンテンツ提供サーバ３は、ユーザ端末２の図示しない表示デバイスに表示するためのエラーメッセージをユーザ端末２へ送信する（ステップＳ２０）。

【００２５】

ステップＳ２３において、コンテンツ提供サーバ３は、ダウンロードユニット１と接続するために、ユーザ端末２をリダイレクトする。

【００２６】

ステップＳ２４において、ダウンロードユニット１は、ユーザ端末２がダウンロードユニット１からスキャンプログラム及び非対称公開鍵をダウンロードできるようにする。

【００２７】

ステップＳ２５において、ユーザ端末２がスキャンプログラム及び非対称公開鍵を記憶した後、ユーザ端末２は、スキャンプログラムを実行し、ハードウェアコンポーネントの識別コードを取得するためにユーザ端末２のハードウェアコンポーネントをスキャンし、取得したハードウェアコンポーネントの識別コードに従って参照ハードウェアスキャンデータを規定する。

【００２８】

参照ハードウェアスキャンデータは、ユーザ端末２と紐づき、また、ユーザ５のユーザ

識別子と一意に対応している。
【００２９】
ステップＳ２６において、ユーザ端末２は、通信ネットワーク１００を介して、参照ハードウェアスキャンデータを各々の識別情報検証サーバ４へ送信し、各々の識別情報検証サーバ４は、ユーザ端末２から受信した参照ハードウェアスキャンデータを記憶する。
【００３０】
図１、３を参照する。ネットワーク認証システムは、好適な実施形態のネットワーク認証方法のログイン処理を実行する。
好適な実施形態のネットワーク認証方法のログイン処理は、次のステップを含む。
【００３１】
ステップ３１において、ユーザ５は、コンテンツ提供サーバ３により提供されるサービスウェブサイト上で、ユーザ端末２のユーザ入力インターフェースを用いて、ユーザＩＤ及びパスワードを入力し、ユーザ端末２は、通信ネットワーク上の第１の通信リンクを介して、ユーザＩＤ及びパスワードを、コンテンツ提供サーバ３へ送信する。
【００３２】
ステップ３２において、ユーザ端末２からのユーザＩＤ及びパスワードの受信に応答して、コンテンツ提供サーバ３は、ユーザＩＤ及びパスワードが正しいか否かチェックする。正しければ、ステップＳ３３に進む。そうでなければ、コンテンツ提供サーバ３は、ユーザ端末２の表示デバイスに表示するためのエラーメッセージを、ユーザ端末２に送信する（ステップＳ３０）。
【００３３】
ステップＳ３３において、コンテンツ提供サーバ３は、ユーザ５の識別情報の検証を要する旨の検証通知を、１つの識別情報検証サーバ４へ送信する。
コンテンツ提供サーバ３は、更に、第１の通信リンクから分離されている第２の通信リンクを介して、当該１つの識別情報検証サーバ４と接続するため、ユーザ端末２をリダイレクトする。
【００３４】
注意されたいのが、ある実施形態においては、当該１つの識別情報検証サーバ４は、コンテンツ提供サーバ３により決定されるが、別の実施形態においては、当該１つの識別情報検証サーバ４は、ユーザ５によって決定される。
【００３５】
更に図４を参照すると、識別情報を検証するための１つの識別情報検証サーバ４が、ユーザ５により決定される手続を示す処理が示されている。
【００３６】
サブステップＳ４１において、コンテンツ提供サーバ３は、各々の識別情報検証サーバ４を表す選択項目のリストを含む選択要求を、ユーザ端末２へ送信する。
【００３７】
コンテンツ提供サーバ３からの選択要求に応答して、ユーザ端末２は、該当する１つの識別情報検証サーバ４を表す、要求された１つの選択項目を示す選択応答を、コンテンツ提供サーバ３へ送信する（サブステップＳ４２）。
【００３８】
したがって、コンテンツ提供サーバ３は、選択応答に従って、識別情報を検証するための該当する１つの識別情報検証サーバ４を決定する（サブステップＳ４３）。
【００３９】
ステップＳ３４において、コンテンツ提供サーバ３からの検証通知の受信に応答して、当該１つの識別情報検証サーバ４は、識別情報検証サーバ４に記憶された暗号化情報のセットを、第２の通信リンクを介して、ユーザ端末２へ送信する。
【００４０】
ステップＳ３５において、当該１つの識別情報検証サーバ４から暗号化情報のセットを受信すると、ユーザ端末２は、暗号化情報のセット及び登録処理のステップＳ２４におい

て記憶した非対称公開鍵に基づき、当該１つの識別情報検証サーバ４が、現在、識別情報を検証するために有効であるか否かを判定する。

【００４１】

ある実施形態においては、ユーザ端末２は、非対称公開鍵を使用し、暗号化情報のセットのうち暗号化されたウェブアドレスを復号する。暗号化されたウェブアドレスの復号が成功すると、ユーザ端末２は、当該１つの識別情報検証サーバ４が、現在、識別情報を検証するために有効であると判定する。そして、ステップ３６に進む。

【００４２】

一方、暗号化情報のうち暗号化されたウェブアドレスの復号が失敗すると、ユーザ端末２によって、当該１つの識別情報検証サーバ４は、現在、識別情報を検証するために有効でないと判断される。このとき、ユーザ端末２は、コンテンツ提供サーバ２に、当該１つの識別情報検証サーバ４が識別情報を検証するために有効でない旨の無効通知を送信する（ステップＳ４０）。

【００４３】

別の実施形態においては、ダウンロードユニット１のデータベースユニットに記憶された、１つの識別情報検証サーバ４に対応する暗号化情報のセットは、更に、その識別情報検証サーバ４に紐づく暗号化された認証期間を含む。

【００４４】

更に図５を参照すると、ステップ３５において、ユーザ端末２が、当該１つの識別情報検証サーバ４が、現在、識別情報を検証するために有効であるか否かを判定する手続を示す処理が示されている。

【００４５】

サブステップＳ５１において、ユーザ端末２は、当該１つの識別情報検証サーバ４の暗号化されたウェブアドレス及び暗号化された認証期間（すなわち、暗号化情報のセット）が、非対称公開鍵を使用して正しく復号されるか否かを判定する。正しく復号されない場合、図３のステップＳ４０に進む。一方、当該１つの識別情報検証サーバ４に紐づく暗号化されたウェブアドレス及び暗号化された認証期間が正しく復号すると、ユーザ端末２は、現在の日付が、当該１つの識別情報検証サーバ４に紐づく復号化された認証期間内か否かを判定する（サブステップＳ５２）。

【００４６】

その結果、認証期間内であれば、ユーザ端末２は、当該１つの識別情報検証サーバ４が、現在、識別情報を検証するために有効であると判断する（ステップＳ５３）。その後、図３のステップＳ３６に進む。

【００４７】

一方、ユーザ端末２は、現在の日付が、当該１つの識別情報検証サーバ４に紐づく復号化された認証期間内ではないと判定した場合、ユーザ端末２は、ダウンロードユニット１に、当該１つの識別情報検証サーバに紐づく認証期間が、既に期限が過ぎている旨の期限切れ通知を送信する（ステップＳ５４）。その後、図３のステップＳ４０に進む。

【００４８】

ステップＳ３６において、ユーザ端末２は、ユーザ端末２のハードウェアコンポーネントをスキャンするためのスキャンプログラムを実行し、ユーザ端末２に紐づくハードウェアスキャンデータとして機能するハードウェアコンポーネントの識別コードを取得し、取得したハードウェアスキャンデータを当該１つの識別情報検証サーバ４へ送信する。

【００４９】

ステップＳ３７において、ユーザ端末２からハードウェアスキャンデータを受信すると、当該１つの識別情報検証サーバ４は、ユーザ端末２に紐づくユーザ５の識別情報を検証するために、ハードウェアスキャンデータとユーザ５の登録処理中に記憶された参照ハードウェアスキャンデータとを比較し、検証結果を、コンテンツ提供サーバ３へ送信する。

【００５０】

ステップＳ３６において取得したハードウェアスキャンデータが、当該１つの識別情報

検証サーバ４に記憶された参照ハードウェアスキャンデータと一致しない場合、検証結果は、ユーザ５の識別情報の検証が失敗した旨を示す。

【００５１】

一方、ステップＳ３６において取得したハードウェアスキャンデータが、当該１つの識別情報検証サーバに記憶された参照ハードウェアスキャンデータと一致した場合、検証結果は、ユーザ５の識別情報の検証が成功した旨を示す。

【００５２】

ステップＳ３８において、コンテンツ提供サーバ３は、当該１つの識別情報検証サーバ４からの検証結果に基づき、ユーザ５の識別情報が認証されたか否かを判定する。

【００５３】

検証結果がユーザ５の識別情報の検証が失敗した旨を示す場合、コンテンツ提供サーバ３によって、ユーザ５の識別情報は認証されないものと判定される。その後、ステップＳ３０へ進む。この場合、ユーザ端末２は、コンテンツ提供サーバ３によって提供されるサービスウェブサイトへのアクセスが拒否される。

【００５４】

一方、検証結果が、ユーザ５の識別情報の検証が成功した旨を示す場合、コンテンツ提供サーバ３によって、ユーザ５の識別情報が認証されたものと判定される。そして、コンテンツ提供サーバ３は、コンテンツ提供サーバ３によって提供されるサービスウェブサイトと接続するため、ユーザ端末２をリダイレクトする（ステップＳ３９）。したがって、ユーザ端末２は、サービスウェブサイトへのアクセスすることを許可される。

【００５５】

要約すると、本発明に係るネットワーク認証方法は以下の利点を有する。

【００５６】

（１）ユーザ端末２は、更なる識別情報の検証のために１つの識別情報検証サーバ４に動的にダイレクトされるため（すなわち、ユーザ端末２は、毎回異なる識別情報検証サーバ４にダイレクトされてもよい）、また、各々の識別情報検証サーバ４に記憶された暗号化情報のセット、及び、ユーザ端末２に記憶された非対称公開鍵は、ダウンロードユニット１からの通知に応答して、必要に応じて不規則に更新されるため、暗号化情報のセットを各々の識別情報検証サーバ４へ提供し、且つ、非対称公開鍵及びスキャンプログラムをユーザ端末２へ提供するダウンロードユニット１を用いた識別情報の検証のための複数認証が達成される。

【００５７】

（２）ユーザ端末２が、ネットワーク認証方法のログイン処理のステップＳ３６を実行する度に、ユーザ端末２は、ハードウェアコンポーネントの識別コードに従ってハードウェアスキャンデータを取得するためにスキャンプログラムを実行する。それゆえ、当該１つの識別情報検証サーバ４によりユーザの識別情報を検証する際に、引き続き使用するため取得されるハードウェアスキャンデータは、動的なデータとなる。

したがって、ネットワークコンテンツプロバイダは識別情報を認証するために追加のデバイスを用意する必要がなく、ダイナミックトークン、ＩＣカード、またはＰＫＩ証明書を有するＵＳＢをユーザへ提供する必要がない。また、ユーザ５も、種々のサービスウェブサイトのための追加の認証デバイスを必要としない。

【００５８】

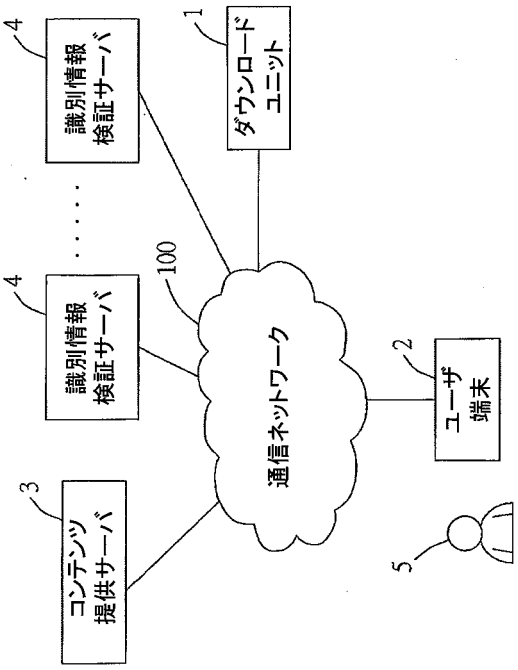
（３）ユーザ端末２は、第１の通信リンクを介して、コンテンツ提供サーバ３と接続し、第２の通信リンクを介して、１つの識別情報検証サーバ４と接続するため、第１の通信リンクと第２の通信リンクを同時に攻撃し、ユーザ端末２によって送信されるデータを盗む（及び／又は改竄する）ことは比較的困難である。

【００５９】

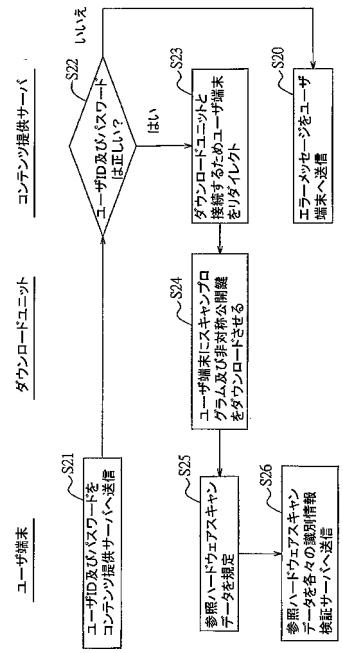
本発明を最も実用的で好ましいと考えられる実施形態に関連して説明したが、本発明は、開示された実施形態に限定されるものではなく、最も広い解釈の精神及び範囲内に含まれる様々な変更例、及び等価な変更例を包含するように意図されていることを理解された

い。

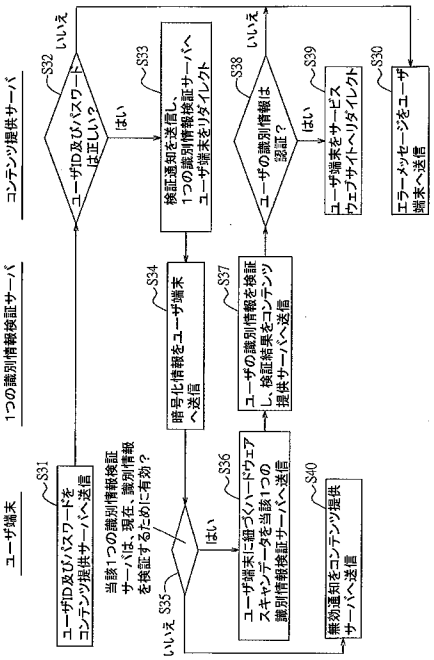
【図１】


4
識別情報
検証サーバ
1
ダウンロード
ユニット
4
識別情報
検証サーバ
100
通信ネットワーク
2
ユーザ
端末
3
コンテンツ
提供サーバ
5

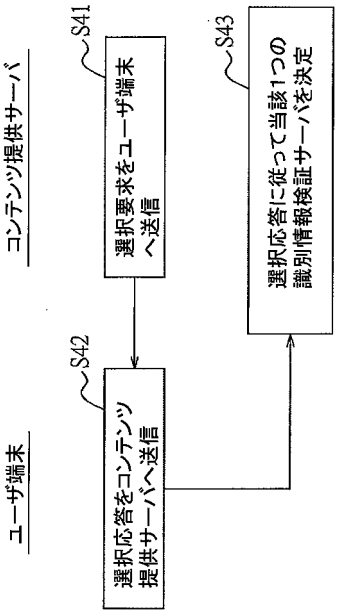
【図２】


ユーザ端末
ダウンロードユニット
コンテンツ提供サーバ
S21
ユーザID及びパスワードを
コンテンツ提供サーバへ送信
S22
ユーザID及びパスワード
は正しい？
いいえ
はい
S20
エラーメッセージをユーザ
端末へ送信
S23
ダウンロードユニットと
接続するためユーザ端末
をリダイレクト
S24
ユーザ端末にスキャングロ
グラム及び非対称公開鍵
をダウンロードさせる
S25
参照ハードウェアスキャン
データを規定
S26
参照ハードウェアスキャン
データを各々の識別情報
検証サーバへ送信

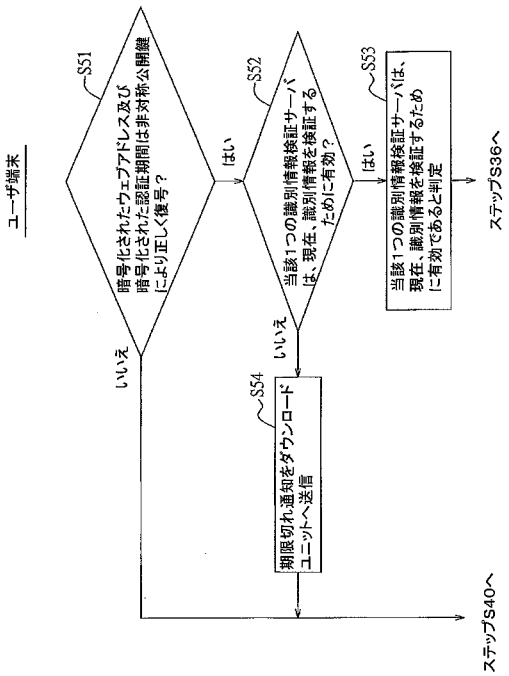
【図３】


ユーザ端末
1つの識別情報検証サーバ
コンテンツ提供サーバ
S31
ユーザID及びパスワードをコンテンツ提供サーバへ送信
当該1つの識別情報検証サーバは、現在、識別情報を検証するために有効？
S32
ユーザID及びパスワードは正しい？
いいえ
はい
S33
検証通知を送信し、1つの識別情報検証サーバへユーザ端末をリダイレクト
S34
暗号化情報をユーザ端末へ送信
S35
いいえ
はい
S36
ユーザ端末に組込ハードウェアスキャンデータを当該1つの識別情報検証サーバへ送信
S37
ユーザの識別情報を検証し、検証結果をコンテンツ提供サーバへ送信
S38
ユーザの識別情報は認証？
いいえ
はい
S39
ユーザ端末をサービスウェブサイトへリダイレクト
S30
エラーメッセージをユーザ端末へ送信
S40
無効通知をコンテンツ提供サーバへ送信

【図４】


ユーザ端末
コンテンツ提供サーバ
S41
選択要求をユーザ端末へ送信
S42
選択応答をコンテンツ提供サーバへ送信
S43
選択応答に従って当該1つの識別情報検証サーバを決定

【図５】


ユーザ端末
S51
暗号化されたウェブアドレス及び暗号化された認証期間は非対称公開鍵により正しく復号？
いいえ
はい
S52
当該1つの識別情報検証サーバは、現在、識別情報を検証するために有効？
いいえ
はい
S53
当該1つの識別情報検証サーバは、現在、識別情報を検証するため有効であると判定
ステップS36へ
S54
期限切れ通知をダウンロードユニットへ送信
ステップS40へ

【外国語明細書】
2015176167000001.pdf